Access Intelligence Information Security Incident Management Policy

All organisations should establish, implement and manage an effective methodology for identifying, investigating, resolving and reviewing all types of "information security incident". As defined within this policy, these are issues affecting the confidentiality, integrity or availability of information assets or the supporting assets upon which information assets may depend for their security.

The essence of this activity is that action should be taken with the urgency required of the incident to (a) stop the incident from escalating and affecting more assets and (b) to bring about a prompt, effective resolution. The existence of an information security incident indicates a need for corrective actions, which as explained in this policy can take a number of different options.

1.0 Policy Objectives

To ensure that Access Intelligence has an effective mechanism in place to promptly identify, report, investigate and resolve information security incidents affecting either information assets, or the supporting assets upon which they may depend (as defined within the Inventory of Assets).

2.0 Policy Scope

Access Intelligence's Information Security Incident Management Policy shall include the following:

- Suspected or actual breaches of confidentiality of an Access Intelligence information asset (or a client data asset where Access Intelligence is engaged in a contractual agreement to protect the client data), or suspected or actual breaches of confidentiality of a supporting asset (upon which the security of information assets depend).

- Suspected or actual breaches of integrity of an Access Intelligence information asset (or a client data asset where Access Intelligence is engaged in a contractual agreement to protect the client data), or suspected or actual breaches of integrity of a supporting asset (upon which the security of information assets depend).

- Suspected or actual interruptions to the availability of an Access Intelligence information asset (or a client data asset where Access Intelligence is engaged in a contractual agreement to protect the client data) from the result of a malicious actor, or suspected or actual interruptions to the availability of a supporting asset (upon which the security of information assets depend) from the result of a malicious actor.

- This Policy shall apply to all employees, contractors and third-party users of Access Intelligence's information systems, and other related infrastructure.

3.0 *Policy Statements*

- An information security incident shall be defined as the suspected or actual breach of confidentiality, integrity or availability of information assets or supporting assets, as defined within the Scope of this Policy.

- The person discovering or suspecting an information security incident shall be responsible for promptly and accurately reporting it. The correct method of reporting an information security incident shall be in person / or on the phone to the Data Protection Officer/Information Security Manager (or a nominated deputy, in their absence).

- All reported information security incidents shall be delivered to and acknowledged by the Data Protection Officer/Information Security Manager (or a nominated deputy, in their absence), who shall take immediate steps to gain a full understanding of the reported incident, validate its actual or potential impact on Access Intelligence, and engage with the Incident Response Team (IRT) and appropriate personnel to investigate and resolve the information security incident.

- If an information security incident indicates a failure or error within an information asset (or supporting asset) risk assessment, then this shall be flagged for an immediate re-assessment to take place by the responsible Asset Owner as a matter of urgency.

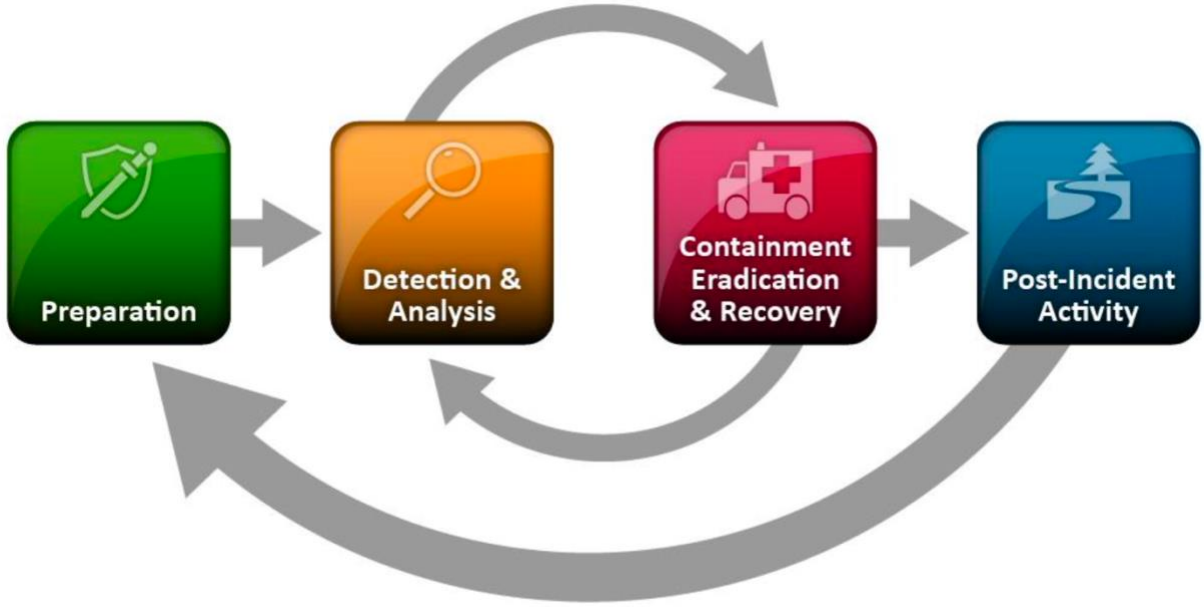
- If an information security incident indicates that a security control is not working effectively, this should either be immediately addressed by the identified Control Owner or, if this cannot be achieved, all Asset Owners that rely upon the affected control should be notified immediately of the potential security risk so that they can make alternative arrangements to suitably protect their own assets.

- Records of the information security incident shall be maintained, including details of the person reporting it, the analysis of the incident, details of the actions implemented, and how the resolved incident was reviewed for effectiveness and formally closed.

- Access Intelligence shall include information security incident statistics as an integral part of Management Review (see **ISDL09**) of the ISMS. Access Intelligence shall understand the root cause of information security incidents and ensure that appropriate corrective actions are implemented to prevent their recurrence. Examples of corrective actions include:

    - Identification of personnel requiring training (and /or disciplinary action)
    - Identification of policies and processes that require strengthening or reworking
    - Identification of failures within the asset's risk assessment that need addressing
    - Identification of weaknesses in security controls that require addressing

4.0 *Incident Response Plan (IRP)*



Source: National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2

4.1 Preparation

Having an established incident response capability is crucial to efficiently manageing security incidents.

- Access Intelligence will establish and maintain an Incident Response Team (IRT) to investigate and respond to security incidents.
- Members of IRT will be responsible for network security and malware prevention.
- Information Security Manager to organise regular Risk Assessments of all Primary and Secondary Information Assets with Asset Owners.
- All staff in scope (See Clause 2.0) will review all Information Security Policies and receive regular information security awareness training

4.2 Detection and Analysis

- IRT Members are responsible for defining common Attack Vectors and organising mitigating actions
- Incidents may be detected through many different means e.g. systems monitoring, vulnerability management, staff/user report
- All suspected or confirmed information security incidents will be reported to the Information Security Manager or IRT member, and logged in the Access Intelligence InfoSec Incident Management (IIM) Board
- The Incident Reporter will be responsible for the initial report
- All suspected or confirmed information security incidents reported to IRT will take immediate priority over any other business

4.3 Containment, Eradication, and Discovery

- The Information Security Manager will triage the Incident Reporters report and categorise the incident:
    1) *Critical* - Organization is no longer able to provide some critical services to any users
    2) *Major* - Organization has lost the ability to provide a critical service to a subset of system users
    3) *Minor* - Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
- The Information Security Manager will organise further investigations into the reported incident and alert IRT members and relevant Asset Owners
- The Incident Response Team will analyse and validate the security incident
- Depending on the security incident:
    .1 Any infected endpoints will be disabled
    .2 Any insider accounts will be blocked

.3 Any breached accounts will have their passwords reset
.4 Relevant backups will be identified and prepared
.5 All evidence to be securely stored
.6 Any improvements to source code or infrastructure will be prioritised

- The IIM Board must be updated with all discoveries and actions
- IRT to provide Asset Owners and Senior Management with regular updates
- Information Security Manager to organise initial notification with relevant external stakeholders within agreed timeframes

4.4 Post-incident Activity

- IRT to communicate *Critical* or *High* incident mitigation to Senior management
- Information Security Manager to organise a detailed incident report with relevant external stakeholders within agreed timeframes, but no later than 1 week after the initial notification
- The incident report will provide the following information where applicable:
  .1 Date and time of incident, date and time of incident discovery and reporting
  .2 Nature of incident; categorisation and description of the data involved
  .3 Description of incident
  .4 Disclosure of any data processors, sub-processors or third parties involved with the breach
  .5 Breakdown of immediate actions and resolutions, including steps to reduce further breaches
  .6 Root cause analysis
  .7 Supervisory Authority notification actions undertaken
  .8 How data subjects have been affected
- Information Security Manager to work with Risk Reporter on documenting Lessons Learnt, and to work with Asset Owners on mitigating reoccurrence
- Information Security Manager to communicate all incidents to Senior Management in regular InfoSec reviews (see ISDL09)

5.0 *Responsibilities*

- The Data Protection Officer/Information Security Manager shall be responsible for:

- Receiving all reported information security incidents
- Performing an initial assessment on the current or potential business impact
- Engaging with resources appropriate to bring about effective closure
- Reporting any security incidents to the relevant Supervisory Authority
  - In the UK, the Information Commissioners Office (ICO) must be notified within 72 hours of Access Intelligence becoming aware of a breach
- If a security incident is likely to result in high risks of adversely affecting individuals' rights and freedoms, where Access Intelligence are acting as a Data Controller, Access Intelligence will also inform those individuals without undue delay, or Access Intelligence will work with the appropriate Data Controller(s) to assist them in fulfilling their GDPR obligations.
- Ensuring that closure activities are appropriate to resolve the information security incident, prevent recurrence, and comply with all Access Intelligence's policies and processes
- Providing statistical information and analysis for Management Review
- Organising information security training, at least once annually, for all staff in scope (see Clause 2.0). Training should include cyber security awareness, how to spot a phishing email, securing remote workstations, amongst other topics (See ISDL2)
- Organising cyber security tests e.g. quizzes, phishing simulations for all staff in scope (see Clause 2.0) and follow up with additional training where required.
- Organise Incident Response simulations

- IRT Members shall we responsible for:
  - Undertaking investigative and resolution actions, as directed by the Information Security Manager or Senior Management, in order to bring about the prompt and effective closure of the information security incident.
  - Search and preserve all evidence, ideally in an encrypted separate location
  - Isolate any infected endpoints from the network
  - Producing appropriate technical detail for internal and external communications
  - Contacting Cyber Insurance Providers and collaborate with any data forensic investigations
  - Maintaining healthy cyber threat intelligence

- Asset Owners, Control Owners and Documentation Owners shall be responsible for:
  - Undertaking investigative and resolution actions, as directed by the Information Security Manager, IRT or Senior Management, in order to

bring about the prompt and effective closure of the information security incident.
    - Vulnerability management of their assigned Information Assets

- The Client Relationship Manager/Account Manager shall be responsible for:

    - Providing a connection between Access Intelligence and the client, should the client be identified as being either responsible (directly or indirectly) for / or affected by the reported information security incident.
    - Providing a connection between Access Intelligence and the client, should the confidentiality, integrity or availability of client information assets (as defined within the Scope of this Policy) be affected by the reported information security incident.

- Senior Management shall be responsible for:

    - Undertaking regular reviews of the performance of the ISMS, including statistics relating to information security incidents, and providing direction and guidance on corrective actions and improvement opportunities that arise from them.

- All staff are responsible for:
    - Reporting suspected and confirmed information security events to the Information Security Manager
    - Reporting asset (and secondary asset) performance issues
    - Completing all assigned Information Security training

All individuals specified within the scope of this Information Security Incident Management Policy (see section 2.0) shall have individual responsibility for complying with every aspect of this policy. The requirement to comply with Access Intelligence policies is included within the Terms and Conditions of Employment and is noted within each individual user's job description. Any failure to adhere to the requirements of this policy shall result in disciplinary action being taken.

6.0 ***Document Version Control***

This policy needs to be reviewed annually as an absolute minimum, or if required changes ae identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this policy, for example because of a reported information security incident, formal review or audit finding.

- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.

- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below.

Version History

Revision	Author	Date	Reason for issue
1.0	David Roud	31/10/2018	First version, to enable Access Intelligence to achieve ISO 27001 accreditation
2.0	Ato Abraham	26/11/2019	Change of leadership team, outsourced IT Service Provider has changed to new company, ISO 27001:2013 certification needs to be renewed
3.0	Adam Palmer	18/01/2021	ISO 27001:2013 certification was renewed in June 2020
4.0	Adam Palmer	31/08/2021	Incident Response Plan (IRP)

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		21/01/2020
Mark Fautley	Chief Financial Officer		20/01/2021

Mark Fautley	**Chief Financial Officer**		**08/09/2021**